Michigan Technological University
Information Technology

Confidentiality Agreement

In accordance with the trust placed in users by the University, employees are responsible for maintaining the confidentiality of the data with which they work and for keeping data secure and accessible only to those who have rights to this information. Faculty and staff members routinely have access to highly sensitive information that could be considered unusual or of interest to other individuals both inside and outside of the University. Because of the sensitive nature of information that is accessible to personnel, all must meet the highest standards possible for managing the University's information in a secure and professional manner.

Every employee is responsible for maintaining the confidentiality of data to which they may have access. Supervisors are responsible for informing employees about policies and procedures, as well as restrictions on confidential information that pertain to their area.

Employees may only use such data as necessary for the purpose for which access has been granted. This includes protecting data from those who do not have authorization to see or access this information. No unauthorized user should see, hear or use user data without proper approval.

Employees also have responsibility for securing data both while it is in use by authorized users and when it is stored (on or offline), printed, faxed or archived, which includes, but is not limited to: appropriate safeguards including locking your workstation when leaving your desk, placing your monitor so that it cannot be viewed by others, deploying privacy screens as necessary, securing mobile devices, and not sharing passwords.

Employees may not disclose this information in any manner of communication, e.g. by file transfer, through written or oral communication, through the unauthorized forwarding of email, or by other means of disclosure without proper authorization.

If at any time data is thought to be compromised, IT should be notified immediately. The intentional act of inappropriately accessing data and information or causing information to be compromised through negligence or failure to appropriately safeguard such information and data may result in disciplinary action, up to and including termination.

University employees are responsible for exercising good judgment in the use of the University's information technology resources.

I understand the information in this document and agree to take the necessary steps to protect the private information of Michigan Tech student, faculty, and staff in accordance with the University's Information Security Plan.